Quantum Attacks without Superposition Queries: The Offline Simon's Algorithm*

Extended Abstract

Xavier Bonnetain[1,3], Akinori Hosoyamada[2,4], María Naya-Plasencia[1], Yu Sasaki[2], and André Schrottenloher[1]

[1] Inria, France
{xavier.bonnetain,maria.naya_plasencia,andre.schrottenloher}@inria.fr
[2] NTT Secure Platform Laboratories, Tokyo, Japan
{hosoyamada.akinori,sasaki.yu}@lab.ntt.co.jp
[3] Sorbonne Université, Collège Doctoral, F-75005 Paris, France
[4] Nagoya University, Nagoya, Japan

Context

Quantum cryptanalysis began with the seminal work of Shor [40], who showed that the RSA and Diffie-Hellman cryptosystems could be broken with a quantum computer. Simon's algorithm [41], which finds a hidden period in $(\{0,1\}^n, \oplus)$, works in a very similar way, but it has been applied in cryptanalysis only recently. In 2010, Kuwakado and Morii [29] showed how to distinguish the three-round Feistel network from a random permutation in quantum polynomial time, if the adversary is allowed to make *superposition queries.* Later on, more results have been obtained in this setting [30, 24, 31].

However, although impressive, these breaks require the *superposition* query model, in which the attacker can access the primitive as a quantum oracle; for example, make quantum encryption queries to a cipher with unknown key.

In this paper, we apply for the first time Simon's algorithm in the standard query model, showing that the aforementioned breaks can have a consequence in this model. This is also the first application of a quantum hidden period algorithm in *symmetric* cryptography with only classical queries. One of our core results is that, while solving a collision search problem with a hidden structure, we can replace a memory of exponential size by $\mathsf{poly}(n)$ qubits. Even though the time speedup remains quadratic, this gives a previously unsuspected advantage to a quantum adversary.

Contributions

We design a quantum algorithm to solve the following problem:

Problem 1 (Asymmetric Search of a Period). Let $F : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^\ell$ and $g : \{0,1\}^n \to \{0,1\}^\ell$ be two functions. We consider F as a family of functions indexed by $\{0,1\}^m$ and write $F(i,\cdot) = f_i(\cdot)$. We are given quantum oracle access to F, and classical or quantum oracle access to g.

* This work was accepted at ASIACRYPT 2019

Assume that there exists exactly one $i \in \{0,1\}^m$ such that $f_i \oplus g$ has a hidden period, *i.e.*: $\forall x \in \{0,1\}^n, f_{i_0}(x) \oplus g(x) = f_{i_0}(x \oplus s) \oplus g(x \oplus s)$ for some s. Furthermore, assume that the other functions are sufficiently "far from being periodic". Then find i_0 and s.

We are not looking for the hidden period of a single boolean function, but for the only periodic function in some search space. Furthermore, this function search space is of the form $\{f_i \oplus g | i \in \{0,1\}^m\}$. Previously, we would have solved this problem using Grover's quantum search [22] among the indices i. This requires to test whether an index i is i_0 or not: we do that by running Simon's boolean hidden shift algorithm [41] on $f_i \oplus g$, which recovers a hidden period, if it exists, with $\mathcal{O}(n)$ superposition queries to f_i and g. In total, this requires $\mathcal{O}\left(n2^{m/2}\right)$ queries *to F and to g* and quantum access to both.

Our new idea is to exploit the "asymmetry" of the problem Assume that we have stored the quantum state: $|\psi_g\rangle := \left(\sum_x |x\rangle |g(x)\rangle\right)^{\otimes cn}$ (where c is a small constant). Assume that we want to compute whether $f \oplus g$ is periodic. By making cn quantum oracle queries to f, we can make the quantum state $|\psi_{f\oplus g}\rangle := \left(\sum_x |x\rangle |(f \oplus g)(x)\rangle\right)^{\otimes cn}$. Then we run Simon's algorithm reversibly and get the information whether $f \oplus g$ has a period. We uncompute back to $|\psi_{f\oplus g}\rangle$, then $|\psi_g\rangle$ by redoing the queries to f. Hence all the queries to g can be made before the Grover search, and $|\psi_g\rangle$ needs to be set up only once.

This new idea leads to a long list of cryptographic applications. In the superposition query model, we can use this algorithm to reduce the amount of queries of many attacks. But we can also obtain new attacks *in the standard query model*. We take the Even-Mansour cipher as an example. It is defined as $E_{k_1,k_2}(x) = k_2 \oplus P(k_1 \oplus x)$ where P is a random permutation. The comparison with previous works is done in Table 1.

Table 1. Previous and New Quantum Attacks on the Even-Mansour cipher (n is the block length, the total key length is $2n$).

Model	Queries	Time	Q-memory	C-memory	Reference
Superposition	$\mathcal{O}(n)$	$\mathcal{O}\left(n^3\right)$	$\mathcal{O}(n)$	$\mathcal{O}\left(n^2\right)$	[30]
Standard	$\mathcal{O}\left(2^{n/3}\right)$	$\mathcal{O}\left(2^{n/3}\right)$	$\mathcal{O}\left(2^{n/3}\right)$	$\mathcal{O}\left(2^{n/3}\right)$	[30]
Standard	$\mathcal{O}\left(2^{3n/7}\right)$	$\mathcal{O}\left(2^{3n/7}\right)$	$\mathcal{O}(n)$	$\mathcal{O}\left(2^{n/7}\right)$	[23]
Standard	$\mathcal{O}\left(2^{n/3}\right)$	$\mathcal{O}\left(n^3 2^{n/3}\right)$	$\mathcal{O}\left(n^2\right)$	$\mathcal{O}(n)$	This paper

Besides the polynomial time attack in the superposition model, Kuwakado and Morii also developed an attack in the standard model with $\mathcal{O}\left(2^{n/3}\right)$ classical queries and $\mathcal{O}\left(2^{n/3}\right)$ quantum RAM [30]. An extension of this attack by Hosoyamada and Sasaki [23] recovers the key with $\mathcal{O}\left(2^{3n/7}\right)$ classical queries, $\mathcal{O}\left(2^{3n/7}\right)$ quantum computations, polynomially many qubits and $\mathcal{O}\left(2^{n/7}\right)$ classical mem-

ory. Our attack in the standard model only uses polynomially many qubits, yet only requires $\mathcal{O}\left(2^{n/3}\right)$ classical queries, $\mathcal{O}\left(n^3 2^{n/3}\right)$ quantum computations and $\mathsf{poly}(n)$ memory.

New Attack on Even-Mansour. We split $k_1 = k_1^{(1)}||k_1^{(2)}$ into $k_1^{(1)}$ of $n/3$ bits and $k_1^{(2)}$ of $2n/3$ bits (Figure 1). We define $g : \{0,1\}^{n/3} \to \{0,1\}^n$ by $g(x) := E_{k_1,k_2}(x\|0^{2n/3})$. Then we can make the quantum state $|\psi_g\rangle$ by classically querying $g(x)$ for *all* $x \in \{0,1\}^{n/3}$. This requires $2^{n/3}$ classical queries. After that, we find $k_1^{(2)}$ using Grover's algorithm. Given a guess $k' \in \{0,1\}^{2n/3}$, we define $f_{k'} : \{0,1\}^{n/3} \to \{0,1\}^n$ by $f_{k'}(x) := P(x\|k')$. Then our guess is correct if and only if the function $f_{k'} \oplus g$ has a period $k_1^{(1)}$. Since $k_1^{(2)}$ can be found in time $\tilde{\mathcal{O}}(2^{n/3})$ with Grover search, we can recover the keys by making $\mathcal{O}(2^{n/3})$ classical queries and $\tilde{\mathcal{O}}(2^{n/3})$ offline quantum computations.

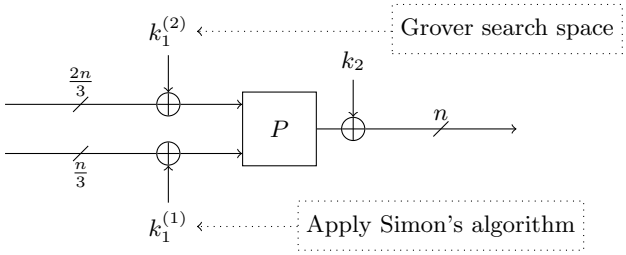

Fig. 1. Attack on the Even-Mansour construction.

Discussion

When the number of classical queries is limited to $2^{n/3}$ (a standard restriction), the best classical attack on Even-Mansour requires finding an n-bit collision between $2^{n/3}$ stored data and some offline queries to the permutation P. Hence, not only does it need $\mathcal{O}\left(2^{2n/3}\right)$ time, but also $\mathcal{O}\left(2^{2n/3}\right)$ accesses to a memory of size $\mathcal{O}\left(2^{n/3}\right)$.

With the same classical data limitation, our algorithm has a time complexity $\mathcal{O}\left(n^3 2^{n/3}\right)$, hence almost a square-root speedup, *and* a memory complexity (quantum and classical) of $\mathcal{O}\left(n^2\right)$. It seems that, by embedding a hidden structure in the memory used, we are able to replace it by the state $|\psi_g\rangle$ defined above. We wonder whether this idea, that we applied to many popular ciphers and modes of encryption, could also prove itself worthy in the context of other quantum algorithms and attacks.

Acknowledgements. The authors thank Léo Perrin for proofreading this article and Elena Kirshanova for helpful remarks. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement n^o 714294 - acronym QUASYModo).

References

1. Albrecht, M.R., Driessen, B., Kavun, E.B., Leander, G., Paar, C., Yalçin, T.: Block ciphers - focus on the linear layer (feat. PRIDE). In: CRYPTO (2). Lecture Notes in Computer Science, vol. 8616, pp. 57–76. Springer (2014)
2. Bertoni, G., Daemen, J., Hoffert, S., Peeters, M., Assche, G.V., Keer, R.V.: Farfalle: parallel permutation-based cryptography. IACR Trans. Symmetric Cryptol. 2017(4), 1–38 (2017), https://tosc.iacr.org/index.php/ToSC/article/view/801
3. Biryukov, A., Wagner, D.A.: Slide attacks. In: FSE. Lecture Notes in Computer Science, vol. 1636, pp. 245–259. Springer (1999)
4. Bonnetain, X.: Quantum key-recovery on full AEZ. In: Selected Areas in Cryptography - SAC 2017. Lecture Notes in Computer Science, vol. 10719, pp. 394–406. Springer (2018)
5. Bonnetain, X., Naya-Plasencia, M.: Hidden shift quantum cryptanalysis and implications. In: ASIACRYPT 2018. Lecture Notes in Computer Science, vol. 11272, pp. 560–592. Springer (2018)
6. Bonnetain, X., Naya-Plasencia, M., Schrottenloher, A.: On quantum slide attacks. In: Selected Areas in Cryptography - SAC 2019. Lecture Notes in Computer Science, Springer (2020)
7. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçin, T.: PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In: ASIACRYPT. Lecture Notes in Computer Science, vol. 7658, pp. 208–225. Springer (2012)
8. Brassard, G., Hoyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. Contemporary Mathematics 305, 53–74 (2002)
9. Brassard, G., Høyer, P., Tapp, A.: Quantum cryptanalysis of hash and claw-free functions. In: Lucchesi, C.L., Moura, A.V. (eds.) LATIN '98: Theoretical Informatics, Third Latin American Symposium, Campinas, Brazil, April, 20-24, 1998, Proceedings. Lecture Notes in Computer Science, vol. 1380, pp. 163–169. Springer (1998), https://doi.org/10.1007/BFb0054319
10. Canteaut, A., Duval, S., Leurent, G., Naya-Plasencia, M., Perrin, L., Pornin, T., Schrottenloher, A.: Saturnin: a suite of lightweight symmetric algorithms for post-quantum security (2019), https://project.inria.fr/saturnin/files/2019/05/SATURNIN- spec.pdf
11. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography 15(2), 125–156 (1998)
12. Chailloux, A., Naya-Plasencia, M., Schrottenloher, A.: An efficient quantum collision search algorithm and implications on symmetric cryptography. In: ASIACRYPT (2). Lecture Notes in Computer Science, vol. 10625, pp. 211–240. Springer (2017)
13. Chakraborti, A., Datta, N., Nandi, M., Yasuda, K.: Beetle family of lightweight and secure authenticated encryption ciphers. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(2), 218–241 (2018), https://doi.org/10.13154/tches.v2018.i2.218-241
14. Crowley, P., Biggers, E.: Adiantum: length-preserving encryption for entry-level processors. IACR Trans. Symmetric Cryptol. 2018(4), 39–61 (2018), https://doi.org/10.13154/tosc.v2018.i4.39-61
15. Daemen, J.: Limitations of the even-mansour construction. In: ASIACRYPT 1991. Lecture Notes in Computer Science, vol. 739, pp. 495–498. Springer (1991)

16. Daemen, J., Hoffert, S., Assche, G.V., Keer, R.V.: The design of xoodoo and xoofff. IACR Trans. Symmetric Cryptol. 2018(4), 1–38 (2018), https://doi.org/10.13154/tosc.v2018.i4.1-38
17. Dinur, I.: Cryptanalytic time-memory-data tradeoffs for fx-constructions with applications to PRINCE and PRIDE. In: EUROCRYPT 2015. Lecture Notes in Computer Science, vol. 9056, pp. 231–253. Springer (2015)
18. Dinur, I., Dunkelman, O., Keller, N., Shamir, A.: Cryptanalysis of iterated even-mansour schemes with two keys. In: ASIACRYPT 2014. Lecture Notes in Computer Science, vol. 8873, pp. 439–457. Springer (2014)
19. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. J. Cryptology 10(3), 151–162 (1997), http://dx.doi.org/10.1007/s001459900025
20. Gagliardoni, T.: Quantum Security of Cryptographic Primitives. Ph.D. thesis, Darmstadt University of Technology, Germany (2017), http://tuprints.ulb.tu-darmstadt.de/6019/
21. Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R.: Applying grover's algorithm to AES: quantum resource estimates. In: PQCrypto. Lecture Notes in Computer Science, vol. 9606, pp. 29–43. Springer (2016)
22. Grover, L.K.: A Fast Quantum Mechanical Algorithm for Database Search. In: Miller, G.L. (ed.) Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996. pp. 212–219. ACM (1996), http://doi.acm.org/10.1145/237814.237866
23. Hosoyamada, A., Sasaki, Y.: Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computations. In: CT-RSA. Lecture Notes in Computer Science, vol. 10808, pp. 198–218. Springer (2018)
24. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: CRYPTO (2). Lecture Notes in Computer Science, vol. 9815, pp. 207–237. Springer (2016)
25. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Quantum differential and linear cryptanalysis. IACR Trans. Symmetric Cryptol. 2016(1), 71–94 (2016), http://tosc.iacr.org/index.php/ToSC/article/view/536
26. Kilian, J., Rogaway, P.: How to protect DES against exhaustive key search. In: CRYPTO. Lecture Notes in Computer Science, vol. 1109, pp. 252–267. Springer (1996)
27. Kuperberg, G.: A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Comput. 35(1), 170–188 (2005), https://doi.org/10.1137/S0097539703436345
28. Kuperberg, G.: Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem. In: TQC 2013. LIPIcs, vol. 22, pp. 20–34. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2013)
29. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round feistel cipher and the random permutation. In: IEEE International Symposium on Information Theory, ISIT 2010, Proceedings. pp. 2682–2685. IEEE (2010)
30. Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012. pp. 312–316. IEEE (2012)
31. Leander, G., May, A.: Grover Meets Simon - Quantumly Attacking the FX-construction. In: ASIACRYPT 2017. Lecture Notes in Computer Science, vol. 10625, pp. 161–178. Springer (2017)

32. Lucchesi, C.L., Moura, A.V. (eds.): LATIN '98: Theoretical Informatics, Third Latin American Symposium, Campinas, Brazil, April, 20-24, 1998, Proceedings, Lecture Notes in Computer Science, vol. 1380. Springer (1998), https://doi.org/10.1007/BFb0054304
33. Martin, L.: XTS: A mode of AES for encrypting hard disks. IEEE Security & Privacy 8(3), 68–69 (2010), https://doi.org/10.1109/MSP.2010.111
34. Mouha, N., Mennink, B., Herrewege, A.V., Watanabe, D., Preneel, B., Verbauwhede, I.: Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In: Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 8781, pp. 306–323. Springer (2014)
35. National Academies of Sciences, Engineering, and Medicine: Quantum Computing: Progress and Prospects. The National Academies Press, Washington, DC (2018), https://www.nap.edu/catalog/25196/quantum-computing- progress-and-prospects
36. National Institute of Standards and Technlology: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process (2016), https://csrc.nist.gov/CSRC/media/ Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf
37. Nielsen, M.A., Chuang, I.: Quantum computation and quantum information. AAPT (2002)
38. Rötteler, M., Steinwandt, R.: A note on quantum related-key attacks. Inf. Process. Lett. 115(1), 40–44 (2015), https://doi.org/10.1016/j.ipl.2014.08.009
39. Sasaki, Y., Todo, Y., Aoki, K., Naito, Y., Sugawara, T., Murakami, Y., Matsui, M., Hirose, S.: Minalpher v1.1. CAESAR competition. (2015), https://competitions.cr.yp.to/round2/minalpherv11.pdf
40. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science. pp. 124–134. IEEE Computer Society (1994)
41. Simon, D.R.: On the Power of Quantum Computation. In: 35th Annual Symposium on Foundations of Computer Science. pp. 116–123 (1994)
42. Winternitz, R.S., Hellman, M.E.: Chosen-key attacks on a block cipher. Cryptologia 11(1), 16–20 (1987), https://doi.org/10.1080/0161-118791861749